(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 944 203 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
22.09.1999 Bulletin 1999/38

(51) Int Cl.[6]: **H04L 12/22**, H04L 29/06, H04Q 7/00, H04L 12/28

(21) Application number: **99660013.6**

(22) Date of filing: **26.01.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **09.02.1998 FI 980291**

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

(72) Inventor: **Turunen, Matti**
33560 Tampere (FI)

(74) Representative: **Johansson, Folke Anders et al**
Nokia Mobile Phones Ltd.,
Intellectual Property Rights,
Keilalahdentie 4
02150 Espoo (FI)

(54) Mobile internet access

(57) A method of enabling roaming of a mobile internet-access host (9) from a local area network (3) to a GSM network (6), each network having a home agent (HA) for routing internet datagrams between networks. The method comprises deregistering the mobile terminal (9) from said local area network (3) and registering it with the GSM network (6) and allocating to the mobile host (9) a new internet address in the GSM network (6). An internet security key is sent via the GSM Short Message Service from the local area network's home agent (HA) to the mobile terminal (9). The new internet address is transmitted, together with authentication data generated using the security key, via the internet (5) to the local area network's home agent (HA) which registers that address as a care-of-address for the mobile host (9).

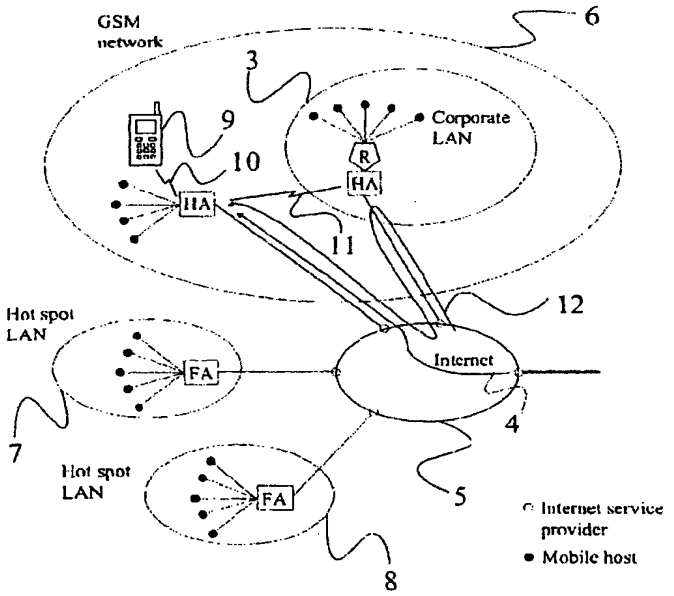

Figure 3

EP 0 944 203 A2

Printed by Jouve, 75001 PARIS (FR)

BNSDOCID: <EP 0944203A2 I >

BEST AVAILABLE COPY

Description

[0001] The present invention relates to mobile internet access and in particular to a method and apparatus for sending a security key to a mobile host for use in internet access.

[0002] Corporate users have traditionally accessed the internet from a fixed location within a Local Area Network (LAN), a user's LAN often being referred to as his "home" network (HN). The user interface to the internet is typically a personal computer (the "host"). As is illustrated in Figure 1. the home network is connected to an internet service provider which routes internet data, so-called "datagrams", between the home network and the internet, the internet in turn comprising other routers and service providers which route data to and from other "foreign" networks (FN).

[0003] In order to be able to transmit and receive datagrams to and from the internet, a host requires an internet address. A corporate home network is typically allocated a set of internet addresses by a national authority and the home network can assign these either fixedly or dynamically to hosts attached to the home network (using for example the Dynamic Host Configuration Protocol DHCP). The allocated set of internet addresses comprise a common prefix portion which identifies the home network, whilst a suffix portion identifies the destination host. When a datagram is received by a home network, a router (R) of the home network polls the attached hosts to determine which host corresponds to the internet address conveyed with the datagram. The datagram is then forwarded by the router to the identified host.

[0004] With the recent rapid advances in mobile communication technology, and in particular of wireless technologies, there has come a desire to gain internet access from mobile hosts or terminals, for example a laptop computer coupled to a cellular telephone. At present, this is available via certain digital telephone networks (e.g. GSM). As with conventional fixed line internet access, a mobile host may have a fixedly or dynamically assigned internet address, allocated by a service provider who is usually the cellular telephone network operator. In the case of mobile internet access, a communication channel between the mobile host and the network is reserved for the duration of the call. Internet data destined for the mobile host is received by the network and is sent to the host over the reserved channel.

[0005] This system works satisfactorily whilst a mobile host remains within one homogeneous network. However, it does not provide for "roaming" between different types of networks or between networks operated by different operators. When a mobile host "de-registers" with one network and registers with a new network, there is no mechanism for forwarding internet datagrams, addressed to the old network, to the new network as the communication channel between the mobile host and the old network no longer exists. It is therefore necessary to open a new communication channel between the mobile host and the new network. All datagrams addressed to the old network and not yet received by the mobile host are lost as a result of this channel change.

[0006] The desire for roaming is likely to increase in the near future as the provision of corporate wireless LANs becomes commonplace. A corporate user will have the opportunity to make wireless voice and data calls from a mobile terminal via the corporate LAN whilst he is inside the coverage area of that LAN. When the user leaves that area, he will then be able to connect to a digital cellular telephone network. In addition, so-called "hot-spot" LANs are likely to be provided in areas where high data capacity is required, e.g. airports, shopping centres. In all probability, hot-spot LANs will be operated by the cellular network operators although they may of course be operated by the property owners themselves.

[0007] A mobile internet access protocol which provides for roaming is currently being standardised by the Internet Engineering Task Force (IETF). This protocol is known as RFC2002. A mobile internet protocol is also described in EP556012. These protocols make use of a "home agent", located in a mobile host's home network, to keep track of the host when it leaves the home network. A mobile host is fixedly allocated an internet address corresponding to the home network.

[0008] When a mobile host is registered to its home network, the functionality of the network's home agent is off for that host (i.e. the host is "deregistered" with the home agent) so that the home agent does not alter the flow of datagrams from the internet to the network's router and the mobile host (as indicated by reference numeral 1 in Figure 2). When the mobile host leaves its home network and contacts a foreign network (FN), the host is registered with a foreign agent (FA) of that network. The foreign agent then transmits to the mobile host an internet address of the foreign agent, and the mobile host in turn transmits the received internet address to the home network's home agent, together with a registration instruction. The home agent registers the new status of the mobile host and records the newly allocated internet address as a "care-of-address" for the host. Whenever the mobile host registers with a new foreign network, a new care-of-address is sent to the home network's home agent to replace the previously registered care-of-address.

[0009] It will be appreciated that, as a mobile host has a fixed internet address allocated to it, datagrams destined for the host will always be sent to the home network. If a mobile host has an active internet connection when it passes from its home network to a foreign network, and a datagram destined for the host subsequently arrives at the home network, the home agent determines that the mobile host is registered with a foreign agent and forwards the datagrams to the registered care-of-address. A communication channel will have

BNSDOCID: <EP _ 0944203A2 I >

been reserved between the mobile host and the foreign agent, and the redirected datagram can be sent to the mobile host over this channel. Similarly, if a mobile host initiates a new internet access when registered with a foreign network, the host continues to use its allocated internet address. The home agent has already received the care-of-address and can again forward datagrams destined for the mobile host to the foreign agent for transfer to the host.

[0010] In some cases, the foreign network may dynamically assign an internet address to a visiting mobile host, e.g. if the foreign network does not have a foreign agent. This address is sent to the mobile host which in turn sends it to the home network's home agent as a care-of-address. Rather than just merely redirecting datagrams to the care-of-address, the home agent actually replaces the old internet address contained in the datagram with the co-located care-of-address before retransmitting the datagram. This particular form of care-of-address which identifies the mobile host as the "tunnel" end-point for the redirected datagrams, rather than a foreign agent, is known as a "co-located care-of-address". It is noted however, that when the mobile host is accessing the internet via the foreign network, it still uses its fixedly allocated internet address. It will therefore be appreciated that regardless of whether the home agent receives a care-of-address or a co-located care-of-address all datagrams directed to a mobile host pass through the home network's home agent (as indicated by reference numeral 2 in Figure 2).

[0011] In a modification to the mobile internet access protocol described above, roaming of a mobile host from a home to a foreign network may be achieved by assigning a new internet address, in said second network, to the mobile host when the host leaves the home network for the foreign network. This new address is then transmitted from the mobile host to the home network's home agent where the new address is registered as a care-of-address or co-located care-of-address for the mobile host. Datagrams addressed to the new internet address are sent directly to the mobile host via the foreign network's "foreign" agent. On the other hand, datagrams addressed to an internet address previously assigned to the mobile host in the home network are forwarded, using the registered care-of-address or co-located care-of-address, from that network's home agent to the mobile host via the foreign network's foreign agent. This protocol is described below with reference to Figure 3.

[0012] Current proposals for mobile internet access protocols have in common the feature that a care-of-address (or co-located care-of-address) must be sent from a mobile host to the host's home network when the host registers with a foreign network. The care-of-address is sent via the internet, together with authentication data generated from an authentication key and the care-of-address itself (or some other component of the registration message), where the secret authentication key is known to the mobile host and to the host's home network. A separate encryption key may also be used to encrypt other data sent between the mobile host and the home network.

[0013] A problem with this approach is that the internet is not necessarily a secure network and it is possible for third parties to intercept internet traffic. If a third party can also determine the authentication/encryption key then it may be possible for them to decrypt intercepted data. It may also be possible for a third party to send a false registration request and care-of-address to a mobile host's home network causing datagrams intended for that mobile host to be redirected to some other terminal.

[0014] A possible way to improve security is to allocate new authentication/encryption keys to a mobile host on a regular basis, e.g. every time the mobile host makes a new internet access request. However, as the new authentication/encryption key is sent via the internet, the possibility remains that each new key may be intercepted and determined.

[0015] It is an object of the present invention to overcome or at least mitigate the above noted disadvantages. In particular, it is an object of the present invention to provide for the secure transmission of security keys, for use in mobile internet access, between a mobile host and a home network of the mobile host, particularly when the mobile host is registered with a foreign network.

[0016] These and other objects are met by sending security keys, from a mobile host's home network to the mobile host, using a point-to-point packet switched service of a cellular radio telephone network.

[0017] According to a first aspect of the present invention there is provided a method of communicating data between a mobile host and a remote station over the internet, where both the mobile host and the remote station are registered with the same or different cellular radio telephone networks, the method comprising the steps of:

sending a security key, from the remote station to the mobile host, over the cellular radio telephone network(s) using a point-to-point packet switched service of the network(s);

receiving said security key at the mobile host, and using the received key to ensure the security of subsequent data transmissions between the mobile host and the remote station over the internet.

[0018] The present invention avoids the use of the internet to distribute a security key to a mobile terminal. Furthermore, distribution is achieved using a cellular radio telephone network messaging service which is inherently more secure than the internet.

[0019] In one embodiment of the present invention, the remote station is connected to a Local Area Network (LAN), the LAN being connected to the internet. The

BNSDOCID: <EP 0944203A2 I >

BEST AVAILABLE COPY

said LAN is assigned as the home network of the mobile host so that said remote terminal is the home agent of the mobile host;
the mobile host is registered with a cellular radio telephone network which provides access for the mobile host to the internet; and
a care-of-address is sent from the mobile host to the home agent over the internet encrypted with said security key.

4. A method according to claim 1, wherein the remote station is the home agent of a cellular telephone network.

5. A method according to claim 4, wherein the remote station is designated as the home agent of the mobile host, as defined by mobile internet protocol.

6. A method according to any one of the preceding claims, wherein the or each cellular radio telephone network is a GSM network and said point-to-point packet switched service is the Short Message Service (SMS).

7. Data communication apparatus comprising:

a mobile host (9) arranged for connection to the internet (5) and to a cellular radio telephone network (6) and having first signal processing means (15) for encrypting and decrypting data sent to and received from the internet (9);
a remote station (HA) arranged for connection to the internet (5) and to a cellular radio telephone network (6), and having second signal processing means (16) for encrypting and decrypting data sent to and received from the internet, the remote station (HA) further comprising means for providing a security key (13) and for sending the security key to the mobile host (9) over the cellular radio telephone network(s) using a point-to-point packet switched service of the network(s);
the mobile host (9) further comprising means for receiving said transmitted security key (14), wherein said security key may be used to secure subsequent data transmissions between the mobile host (9) and the remote station (HA) over the internet (5).

BEST AVAILABLE COPY

BNSDOCID: <EP 0944203A2 I >

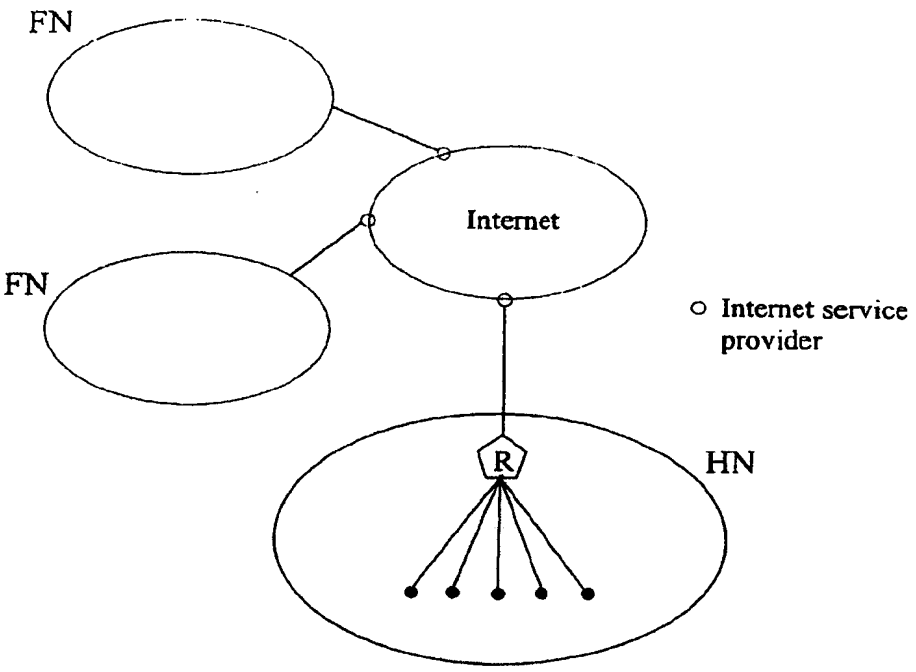

Figure 1

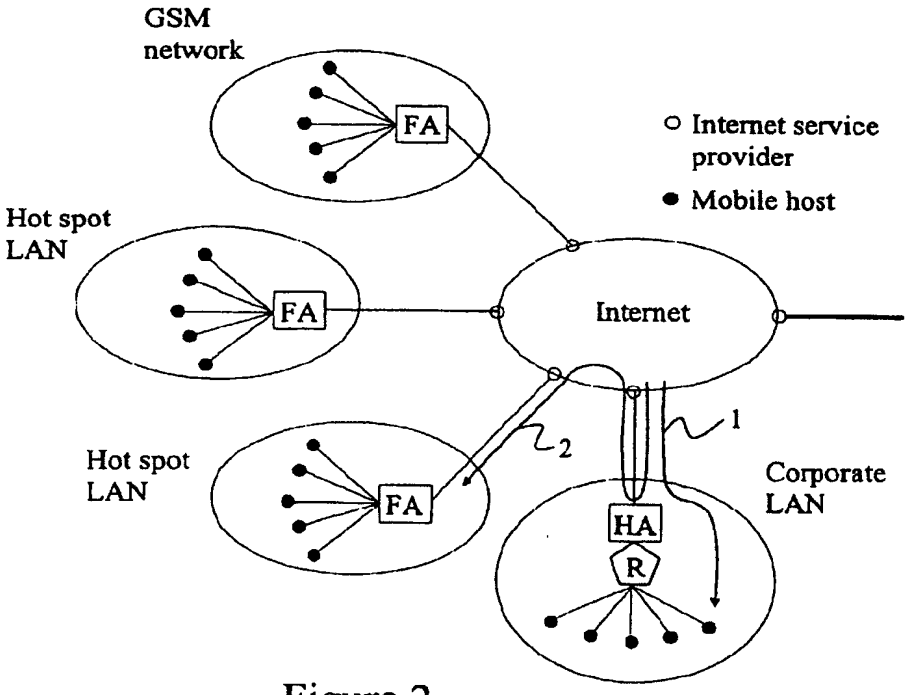

Figure 2

BEST AVAILABLE COPY

BNSDOCID: <EP 0944203A2 I >

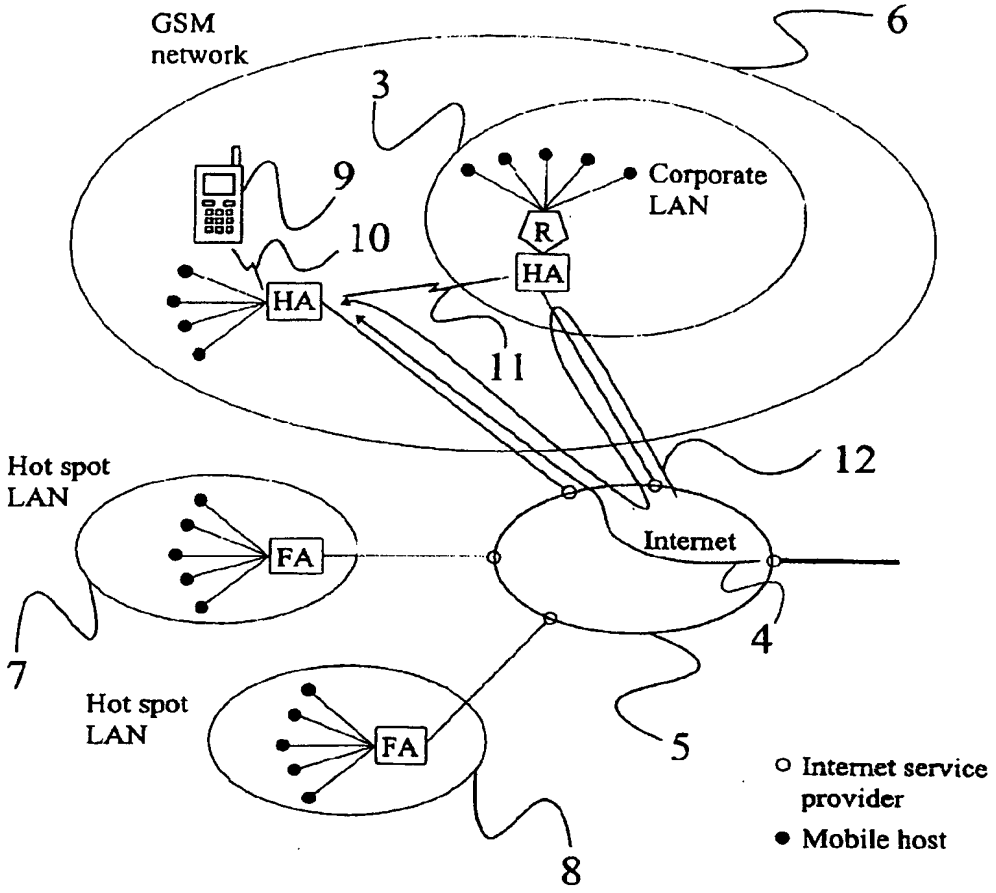

Figure 3

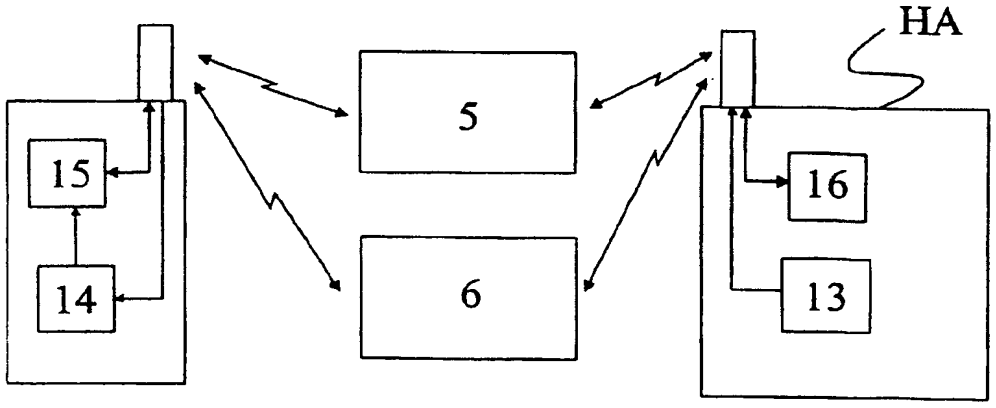

Figure 4

BEST AVAILABLE COPY

BNSDOCID: <EP 0944203A2 I >

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 944 203 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
10.01.2001 Bulletin 2001/02

(43) Date of publication A2:
22.09.1999 Bulletin 1999/38

(21) Application number: **99660013.6**

(22) Date of filing: **26.01.1999**

(51) Int Cl.[7]: **H04L 12/22**, H04L 29/06, H04Q 7/00, H04L 12/28

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **09.02.1998 FI 980291**

(71) Applicant: **NOKIA MOBILE PHONES LTD.**
02150 Espoo (FI)

(72) Inventor: **Turunen, Matti**
33560 Tampere (FI)

(74) Representative: **Johansson, Folke Anders et al**
Nokia Corporation,
P.O. Box 319
00045 Nokia Group (FI)

(54) Mobile internet access

(57) A method of enabling roaming of a mobile internet-access host (9) from a local area network (3) to a GSM network (6), each network having a home agent (HA) for routing internet datagrams between networks. The method comprises deregistering the mobile terminal (9) from said local area network (3) and registering it with the GSM network (6) and allocating to the mobile host (9) a new internet address in the GSM network (6). An internet security key is sent via the GSM Short Message Service from the local area network's home agent (HA) to the mobile terminal (9). The new internet address is transmitted, together with authentication data generated using the security key, via the internet (5) to the local area network's home agent (HA) which registers that address as a care-of-address for the mobile host (9).

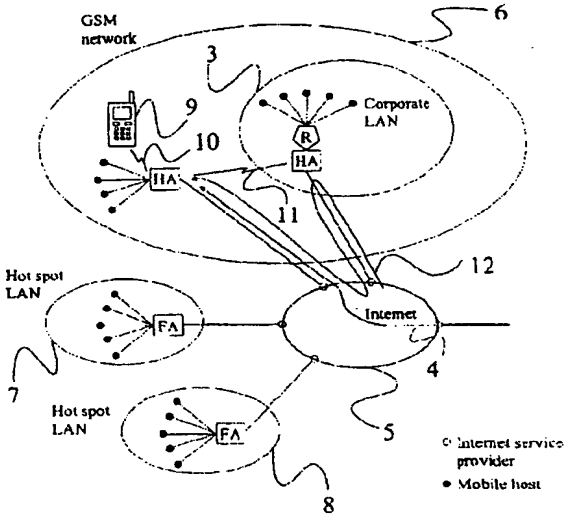

Figure 3

EP 0 944 203 A3

Printed by Jouve, 75001 PARIS (FR)

BEST AVAILABLE COPY

BNSDOCID: <EP 0944203A3 I >

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 66 0013

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	C PERKINS: "RFC 2002: IP Mobility Support" RFC 2002, October 1996 (1996-10), XP002123919 IBM, US	1,6	H04L12/22 H04L29/06 H04Q7/00 H04L12/28
A	* page 5, line 4 - page 70, line 12 *	7	
Y	WO 97 31306 A (NOKIA) 28 August 1997 (1997-08-28)	1,6	
A	* page 5, line 32 - page 9, line 37; figures *	7	
A	WO 97 04611 A (ERICSSON) 6 February 1997 (1997-02-06) * page 8, line 14 - page 38, line 21; figures *	1-7	
A	PERKINS C E: "MOBILE IP" IEEE COMMUNICATIONS MAGAZINE,IEEE SERVICE CENTER. PISCATAWAY, N.J,US, vol. 35, no. 5, 1 May 1997 (1997-05-01), pages 84-86,91-99, XP000657114 ISSN: 0163-6804 * see complete article *	1-7	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04Q
A	EP 0 483 547 A (IBM) 6 May 1992 (1992-05-06) * page 3, column 4, line 19 - page 7, column 11, line 39; figures *	1,7	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 November 2000	Geoghegan, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BEST AVAILABLE COPY

BNSDOCID: <EP ... 0944203A3 I >

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 66 0013

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-11-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9731306 A	28-08-1997	FI 960820 A	24-08-1997
		AU 1604497 A	10-09-1997
		EP 0976015 A	02-02-2000
		US 6112078 A	29-08-2000
WO 9704611 A	06-02-1997	US 5825759 A	20-10-1998
		AU 707478 B	08-07-1999
		AU 6839896 A	18-02-1997
		CA 2227556 A	06-02-1997
		CN 1196153 A	14-10-1998
		EP 0840986 A	13-05-1998
		JP 2000502521 T	29-02-2000
EP 483547 A	06-05-1992	US 5159592 A	27-10-1992
		DE 69119353 D	13-06-1996
		DE 69119353 T	07-11-1996
		JP 2516291 B	24-07-1996
		JP 4227149 A	17-08-1992

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BEST AVAILABLE COPY

BNSDOCID: <EP 0944203A3 I >